IEEE Xplore RELEASE 2.1

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

☐ Search Session History BROWSE SEARCH IEEE XPLORE GUIDE

Wed, 8 Nov 2006, 4:28:00 PM EST

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Search Query Display

Recent Search Queries

#1	((kasumi <in>metadata) <and> (3gpp<in>metadata))
#2	(kasumi<in>metadata)
#3	kasumi
#4	(speed<IN>metadata)
#5	kasumi
#6	((kasumi)<AND>(speed<in>metadata))
#7	(Kasumi and parallel processing<IN>metadata)
#8	(Kasumi and parallel processing<IN>metadata)
#9	(kasumi feal <and>parallel compution)
#10	((kasumi or feal <and>parallel computino)<IN>metadata)
#11	((kasumi or feal <and>parallel compution)<in>metadata)
#12	((kasumi or feal <and>parallel compution)<in>metadata)
#13	((cipher* or encryp*<in>au) <and> (speeed <in>metadata)) <and> (reduce production cost<in>metadata)
#14	((cipher* or encryp*<in>au) <and> (speeed <in>metadata)) <and> (reduce production cost<in>metadata)
#15	((cipher* or encryp*<in>au) <and> (speeed <in>metadata)) <and> (reduce production cost<in>metadata)
#16	(kasumi<and>parallel)<and>comutation or processing
#17	((kasumi<and>parallel)<and>(comutation or processing) <IN>metadata)
#18	((kasumi<and>parallel)<and>(comutation or processing) <IN>metadata)

#19 (kasumi) <and> (pyr >= 2000 <and> pyr <= 2002)

#20 ((kasumi) <and> (pyr >= 1990 <and> pyr <= 2002) <IN>metadata)

#21 (fast implementation of secret-key bloack cipher<in>metadata)

#22 (mixed inner*<in>ti)

#23 (chodowiec<in>au)

Help Contact Us Privacy &

Indexed by Inspec®

© Copyright 2006 IEEE –

IEEE Xplore RELEASE 2.1

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

Search Results BROWSE SEARCH IEEE XPLORE GUIDE

Results for "((kasumi or feal <and>parallel compution)<in>metadata)" e-mail
Your search matched **10** of **1430374** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((kasumi or feal <and>parallel compution)<in>metadata) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **High-speed hardware implementations of the KASUMI block cipher**
Kitsos, P.; Galanis, M.D.; Koufopavlou, O.;
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 2, 23-26 May 2004 Page(s):II - 549-52 Vol.2
AbstractPlus | Full Text: PDF(258 KB) IEEE CNF
Rights and Permissions

2. **A methodology for dynamic power consumption estimation using VHDL**
Alcantara, J.M.S.; Vieira, A.C.C.; Galvez-Durand, F.; Alves, V.C.;
Integrated Circuits and Systems Design, 2002. Proceedings. 15th Symposium
9-14 Sept. 2002 Page(s):149 - 154
Digital Object Identifier 10.1109/SBCCI.2002.1137651
AbstractPlus | Full Text: PDF(1165 KB) IEEE CNF
Rights and Permissions

3. **Leveraging the Multiprocessing Capabilities of Modern Network Processe Cryptographic Acceleration**
Gaubatz, G.; Sunar, B.;
Network Computing and Applications, Fourth IEEE International Symposium o
27-29 July 2005 Page(s):235 - 238
Digital Object Identifier 10.1109/NCA.2005.28
AbstractPlus | Full Text: PDF(200 KB) IEEE CNF
Rights and Permissions

4. **ASC: a stream compiler for computing with FPGAs**
Mencer, O.;
Computer-Aided Design of Integrated Circuits and Systems, IEEE Transaction
Volume 25, Issue 9, Sept. 2006 Page(s):1603 - 1617
Digital Object Identifier 10.1109/TCAD.2005.857377
AbstractPlus | Full Text: PDF(360 KB) IEEE JNL
Rights and Permissions

5. **High performance encryption cores for 3G networks**
Balderas-Contreras, T.; Cumplido, R.;
Design Automation Conference, 2005. Proceedings. 42nd
13-17 June 2005 Page(s):240 - 243
AbstractPlus | Full Text: PDF(198 KB) IEEE CNF

Rights and Permissions

6. **Design and implementation of Rijndael algorithm for GSM encryption**
Soyjaudah, K.M.S.; Hosany, M.A.; Jamaloodeen, A.;
Mobile Future, 2004 and the Symposium on Trends in Communications. Symp IST Workshop on
24-26 Oct. 2004 Page(s):106 - 109
Digital Object Identifier 10.1109/TIC.2004.1409510
AbstractPlus | Full Text: PDF(660 KB) IEEE CNF
Rights and Permissions

7. **An end-to-end hardware approach security for the GPRS**
Kitsos, P.; Sklavos, N.; Koufopavlou, O.;
Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12th Mediterranean
Volume 2, 2004 Page(s):791 - 794 Vol.2
Digital Object Identifier 10.1109/MELCON.2004.1347050
AbstractPlus | Full Text: PDF(463 KB) IEEE CNF
Rights and Permissions

8. **Design space exploration with A Stream Compiler**
Mencer, O.; Pearce, D.J.; Howes, L.W.; Luk, W.;
Field-Programmable Technology (FPT), 2003. Proceedings. 2003 IEEE Interna Conference on
15-17 Dec. 2003 Page(s):270 - 277
AbstractPlus | Full Text: PDF(532 KB) IEEE CNF
Rights and Permissions

9. **Design and implementation of a private and public key crypto processor application to a security system**
Ho Won Kim; Sunggu Lee;
Consumer Electronics, IEEE Transactions on
Volume 50, Issue 1, Feb 2004 Page(s):214 - 224
Digital Object Identifier 10.1109/TCE.2004.1277865
AbstractPlus | Full Text: PDF(1093 KB) IEEE JNL
Rights and Permissions

10. **An efficient reuse-based approach to implement the 3GPP KASUMI block**
Balderas-Contreras, T.; Cumplido-Parra, R.A.;
Electrical and Electronics Engineering, 2004. (ICEEE). 1st International Confe
24-27 June 2004 Page(s):113 - 118
Digital Object Identifier 10.1109/ICEEE.2004.1433860
AbstractPlus | Full Text: PDF(295 KB) IEEE CNF
Rights and Permissions

Help Contact Us Privacy &
Indexed by Inspec
© Copyright 2006 IEEE –

PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+KASUMI speed performance
SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used **KASUMI speed performance** Found **7** of **189,785**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 7 of 7

Relevance scale

1 Survey and benchmark of block ciphers for wireless sensor networks

Yee Wei Law, Jeroen Doumen, Pieter Hartel
February 2006 **ACM Transactions on Sensor Networks (TOSN)**, Volume 2 Issue 1
Publisher: ACM Press
Full text available: pdf(354.39 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without human intervention for a long period of time with little energy supply, and that available storage is scarce on these sensor nodes. However, to our knowledge, no systematic work has been done in this area so far. We construct an evaluation framew ...

Keywords: Sensor networks, block ciphers, cryptography, energy efficiency

2 Architectures for cryptography and security applications: High performance encryption cores for 3G networks

Tomás Balderas-Contreras, René Cumplido
June 2005 **Proceedings of the 42nd annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(869.33 KB) Additional Information: full citation, abstract, references, index terms

This paper presents two novel and high performance hardware architectures, implemented in FPGA technology, for the KASUMI block cipher; this algorithm lies at the core of the confidentiality and integrity algorithms defined for the Universal Mobile Telecommunication System (UMTS) standard. The first proposal is a pipelined design and the second implements an iterative approach. The throughput for these architectures turn out to be higher than the throughput achieved by other proposals.

Keywords: 3G, FPGA, KASUMI, UMTS security architecture

3 Special session on security on SoC: Securing wireless data: system architecture challenges

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally
October 2002 **Proceedings of the 15th international symposium on System Synthesis**

Publisher: ACM Press

Full text available: pdf(172.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview of emerging techniques to address them. We focus on the computational requirements for securing wireless data transactions, revealing a gap between these requirements and the trends in processing capabilities of embedded processors used in wireless h ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

4 Taming the IXP network processor

Lal George, Matthias Blume

May 2003 **ACM SIGPLAN Notices , Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation PLDI '03**, Volume 38 Issue 5

Publisher: ACM Press

Full text available: pdf(159.27 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We compile Nova, a new language designed for writing network processing applications, using a back end based on integer-linear programming (ILP) for register allocation, optimal bank assignment, and spills. The compiler's optimizer employs CPS as its intermediate representation; some of the invariants that this IR guarantees are essential for the formulation of a practical ILP model.Appel and George used a similar ILP-based technique for the IA32 to decide which variables reside in registers but ...

Keywords: Intel IXA, bank assignment, code generation, integer linear programming, network processors, programming languages, register allocation

5 Dynamic Platform Management for Configurable Platform-Based System-on-Chips

Krishna Sekar, Kanishka Lahiri, Sujit Dey

November 2003 **Proceedings of the 2003 IEEE/ACM international conference on Computer-aided design**

Publisher: IEEE Computer Society

Full text available: pdf(330.64 KB) Additional Information: full citation, abstract, index terms

General-purpose System-on-Chip platforms consistingof configurable components are emerging as an attractivealternative to traditional, customized solutions (e.g., ASICs,custom SoCs), owing to their flexibility, time-to-market advantage,and low engineering costs. However, the adoptionof such platforms in many high-volume markets (e.g, wirelesshandhelds) is limited by concerns about their performance andenergy-efficiency. This paper addresses the problemof enablingthe use of configurable platforms ...

6 Document exchange model for augmenting added value of B2B collaboration

Koichi Hayashi, Riichiro Mizoguchi

September 2003 **Proceedings of the 5th international conference on Electronic commerce ICEC '03**

Publisher: ACM Press

Full text available: pdf(148.98 KB) Additional Information: full citation, abstract, references

In this paper we present a B2B integration project, which aims to augment the added value of services instead of improving efficiency by automating processes. This paper introduces the VAlue Layered docUment Exchange (VALUE) model, which is a novel collaboration model adopted for this project. The key feature of the VALUE model is that partners exchange XML documents that are updated by adding elements for process information, such as the acceptance or rejection of a proposal, to received docume ...

Keywords: B2B, ebXML, supply chain management

7 A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation

Kris Tiri, Ingrid Verbauwhede

February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1**

Publisher: IEEE Computer Society

Full text available: pdf(143.96 KB) Additional Information: full citation, abstract, citings, index terms

This paper describes a novel design methodology to implement a secure DPA resistant crypto processor. The methodology is suitable for integration in a common automated standard cell ASIC or FPGA design flow. The technique combines standard building blocks to make new'compound standard cells, which have a close to constant power consumption. Experimental results indicate a 50 times reduction in the power consumption fluctuations.

Results 1 - 7 of 7

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player